

CHARACTERIZATION OF 2-RAMIFIED POWER SERIES

JONAS FRANSSON

Department of Mathematics, Linnæus University, Växjö, Sweden

ABSTRACT. In this paper we study lower ramification numbers of power series tangent to the identity that are defined over fields of positive characteristics p . Let g be such a series, then g has a fixed point at the origin and the corresponding lower ramification numbers of g are then, up to a constant, the degree of the first non-linear term of p -power iterates of g . The result is a complete characterization of power series g having ramification numbers of the form $2(1 + p + \cdots + p^n)$. Furthermore, in proving said characterization we explicitly compute the first significant terms of g at its p th iterate.

Keywords: Lower ramification numbers, iterations of power series, difference equations, arithmetic dynamics

1. INTRODUCTION

Iteration of power series is an important part of arithmetic dynamics [Sil07, AK09, Shp07], which is a very active area of research within the general field of dynamical systems. In this article we are interested in power series defined over fields of positive characteristic p . In particular, the degree of the first non-linear term of p -power iterates of power series tangent to the identity, the so called lower ramification numbers of such series. Recent results by Lindahl and Rivera-Letelier [Lin13, LRL16a, LRL16b] show that there is a connection between the geometric location of periodic points of power series over ultrametric fields and lower ramification numbers.

Throughout the paper let p be a prime number and k a field of characteristic p , also let $g \in k[[\zeta]]$ be a power series of the form

$$(1.1) \quad g(\zeta) = \zeta + \cdots .$$

The *order* of a nonzero power series g is the lowest degree of its non-zero terms and we denote this by $\text{ord}(\cdot)$. We put $\text{ord}(0) := +\infty$. Let $g^n(\zeta)$ denote the n -fold composition of itself. The *lower ramification number* i_n of a power series g is defined as

$$(1.2) \quad i_n(g) := \text{ord} \left(\frac{g^{p^n}(\zeta) - \zeta}{\zeta} \right) .$$

E-mail address: jonas.fransson@lnu.se.

A famous theorem of Sen [Sen69],ⁱ often referred to as Sen's theorem, states that if $g^m \neq \text{Id}$, for all integers $m \geq 1$ then

$$i_n(g) \equiv i_{n-1}(g) \pmod{p^n}.$$

Given $i_0(g) = 1$ we then have

$$(1.3) \quad i_n(g) \geq 1 + p + \cdots + p^n.$$

Rivera-Letelier [RL03, Example 3.19] gave a complete characterization of power series for which (1.3) holds with equality. Keating [Kea92] proved a similar result for the special case that $p = 3$.

Definition 1. *Let p be a prime and k a field of characteristic p . Furthermore, let g be a power series in $k[[\zeta]]$. Then g is said to be 2-ramified if its sequence of lower ramification numbers is of the form*

$$(1.4) \quad i_n(g) = 2(1 + p + \cdots + p^n).$$

In this paper we give a complete characterization of all power series of the form (1.1) for which Definition 1 is satisfied.

Theorem 1. *Let p be an odd prime and let k be a field of characteristic p . Let $g \in k[[\zeta]]$ be a power series of the form*

$$g(\zeta) = \zeta \left(1 + \sum_{j=1}^{+\infty} a_j \zeta^j \right).$$

Then g is 2-ramified if and only if $a_1 = 0$, $a_2 \neq 0$ and

$$(1.5) \quad 3/2a_2^3 + a_3^2 - a_2a_4 \neq 0.$$

Remark 1. Note that for $p = 2$, g can be written of the form $\zeta + a_2\zeta^{p+1} + \cdots$, which implies $i_0(g) = p$. From [LS98, Corollary 1] we know that if p divides $i_0(g)$ then $i_n(g) = i_0(g)p^n$ for all integers $n \geq 0$. Therefore, Theorem 1 is only stated for odd primes.

Our primary technical result is the computation of the first significant terms of the p th iterate of g .

Proposition 1. *Let p be a prime and k field of characteristic p . Let $g \in k[[\zeta]]$ be a power series of the form*

$$g(\zeta) = \zeta (1 + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4) \pmod{\langle \zeta^6 \rangle},$$

then

$$(1.6) \quad g^p(\zeta) - \zeta \equiv a_2^{p-2} (3/2a_2^3 + a_3^2 - a_2a_4) \zeta^{2p+3} \pmod{\langle \zeta^{2p+4} \rangle}.$$

In combination with the following result from Laubie and Saïne this computation yields sufficient information to prove Theorem 1.

ⁱAlternative proofs are given in [Lub95, LRL16b].

Lemma 1 ([LS98], Corollary 1). *Let p be a prime and k be a field of characteristic p . Moreover, let $g \in k[[\zeta]]$, be a power series of the form (1.1). If $p \nmid i_0(g)$ and $i_1(g) < (p^2 - p + 1)i_0(g)$, then*

$$i_n(g) = i_0(g) + \frac{p^n - 1}{p - 1}(i_1(g) - i_0(g)),$$

for all integers $n \geq 0$.

Lemma 1 is a restatement of the last statement of Corollary 1 in [LS98].

Our approach of calculating the p th iterate of g given in Proposition 1 is similar to methods used in [LRL16a, LRL16b]. Proofs of Theorem 1 and Proposition 1 will be given in §3.

1.1. Implication. In [LRL16a, LRL16b] the authors study the relation between the lower ramification numbers and the geometric location of periodic points of ultrametric dynamical systems. In their results several important discoveries concerning lower ramification numbers have been made. The authors are especially interested in parabolic power series not necessarily tangent to the identity. Let $\gamma \in k$ such that $\gamma^q = 1$, and $f \in k[[\zeta]]$, be a power series of the form $f(\zeta) = \gamma\zeta + \dots$. Then f is said to be *minimally ramified*ⁱⁱⁱ if

$$i_n(f^q) = q(1 + p + \dots + p^n).$$

In [LRL16a, Theorem C] a characterization of minimally ramified power series is given. However, for the case that $\gamma = -1$, i.e. $q = 2$, minimal ramification corresponds to 2-ramification, in the sense that f is minimally ramified if and only if f^2 is 2-ramified. This implies that Theorem 1 provides an alternative proof for this special case, where $f^2 = g$. In fact straightforward computation yields the following corollary from Theorem 1.

Corollary 1. *Let p be an odd prime and k a field of characteristic p . Furthermore let $f \in k[[\zeta]]$ be of the form*

$$f(\zeta) = \zeta \left(-1 + \sum_{j=1}^{+\infty} a_j \zeta^j \right).$$

Then $f^2(\zeta)$ is 2-ramified if and only if

$$(a_1^2 + a_2)(11a_1^4 + 25a_1^2a_2 + 12a_1a_3 + 6a_2^2 + 4a_4) \neq 0$$

The proof of this corollary follows from Theorem 1 and is given in §3.1, and a consequence of the corollary is the following interesting example.

Example 1. *Let p be an odd prime and k a field of characteristic p . Let $f \in k[\zeta]$ be the polynomial $f(\zeta) = -\zeta + \zeta^2$, then f^2 is 2-ramified if and only if $p \neq 11$.*

ⁱⁱⁱThe notion of minimal ramification was first introduced for wildly ramified automorphisms, i.e. $\gamma = 1$ by [LMS02] where it corresponds to ramification numbers of the form $1 + p + \dots + p^n$.

1.2. Related works. The relation between lower ramification numbers and arithmetic dynamics over ultrametric fields is one of the motivations for this study. However, ramification numbers have also been considered in different contexts. In the study of the potential sequences of ramification numbers, Keating [Kea92] used the relation between the ramification numbers and abelian extensions of $k((t))$. Laubie and Saïne [LS97, LS98] could later improve these results by applying Wintenberger's theory on fields of norms [Win04]. In [LMS02] the authors study Lubin's conjecture [Lub94], on the relation between wildly ramified power series and formal groups.

1.3. Acknowledgments. I would like to thank Karl-Olof Lindahl for fruitful discussions and support during this work, and for introducing me to the topic. His comments and guidance certainly helped me improve the presentation, and clear my thoughts about these matters. I would also like to thank Juan Rivera-Letelier and the referee for helpful comments on the paper.

2. PRELIMINARIES

Given a ring R and an element $a \in R$ we let $\langle a \rangle$ denote the ideal of R generated by a .

Throughout the paper for any nonnegative integer n let $n!!$ denote the *double factorial* of n . Let $0!! = 1!! = 1$, and for integers $n \geq 2$, we have

$$n!! = n(n-2)!!.$$

Let $(k, |\cdot|)$ be an ultrametric field, and let \mathcal{O}_k denote the ring of integers of k , and \mathfrak{m}_k its maximal ideal. Let $\tilde{k} := \mathcal{O}_k/\mathfrak{m}_k$ be the residue field of k . Furthermore, denote the projection in \tilde{k} of an element a of \mathcal{O}_k by \tilde{a} ; it is the reduction of a . The reduction of a power series $g \in \mathcal{O}_k[[\zeta]]$ is the power series $\tilde{g}(\zeta) \in \tilde{k}[[\zeta]]$ whose coefficients are the reductions of the corresponding coefficients of g . Moreover, let \mathbb{Q}_p be the p -adic numbers and let \mathbb{Z}_p denote its ring of integers.

3. CHARACTERIZATION OF 2-RAMIFIED POWER SERIES

In this section we prove our main results. As mentioned in the introduction Theorem 1 is a consequence of Proposition 1, which also will be proved within this section. However, to prove this in turn we will need several lemmas and the proofs of Theorem 1 and Proposition 1 will follow thereafter.

Lemma 2. *Let p be an odd prime. For each integer $n \geq 1$ let \mathcal{R}_n and \mathcal{T}_n in \mathbb{Q}_p be defined by*

$$(3.1) \quad \mathcal{R}_n := (2n-1)!! \sum_{r=1}^n \left[\prod_{j=r+1}^n \frac{2j}{2j-1} \right],$$

and

$$(3.2) \quad \mathcal{T}_n := (2n+1)!! \sum_{j=1}^n \frac{(2j)!!}{(2j+1)!!}.$$

Then

$$\mathcal{R}_n = (2n+1)!! - (2n)!! \text{ and } \mathcal{T}_n = (2n+2)!! - 2(2n+1)!!.$$

Moreover, $\widehat{\mathcal{R}}_p = \widehat{\mathcal{T}}_p = 0$.

Proof. The last consequence of the lemma follows from the first by simply putting $n = p$.

Proof of \mathcal{R}_n . We proceed by induction in n to see that the identity is valid. For $n = 2$ it holds and we prove that it holds for arbitrarily chosen n , but first note that

$$\sum_{r=1}^n \left[\prod_{j=r+1}^n \frac{2j}{2j-1} \right] = \sum_{r=1}^n \frac{(2n)!!(2r-1)!!}{(2n-1)!!(2r)!!}.$$

Now we proceed by induction in n and study $n+1$

$$\begin{aligned} \sum_{r=1}^{n+1} \frac{(2n+2)!!(2r-1)!!}{(2n+1)!!(2r)!!} &= \frac{(2n+2)!!(2n+1)!!}{(2n+1)!!(2n+2)!!} + \sum_{r=1}^n \frac{(2n+2)!!(2r-1)!!}{(2n+1)!!(2r)!!} \\ &= 1 + \frac{2n+2}{2n+1} \sum_{r=1}^n \frac{(2n)!!(2r-1)!!}{(2n-1)!!(2r)!!} \\ &\stackrel{\text{IA}}{=} 1 + \frac{2n+2}{2n+1} \left((2n+1) - \frac{(2n)!!}{(2n-1)!!} \right) \\ &= 1 + (2n+2) - \frac{(2n+2)!!}{(2n+1)!!} \\ &= (2n+3) - \frac{(2n+2)!!}{(2n+1)!!}, \end{aligned}$$

by multiplying with $(2n+1)!!$ we get the proposed identity.

Proof of \mathcal{T}_n . A straightforward computation shows that the identity holds for $n = 1$. We proceed by induction in n . Assume that the lemma holds for $n \geq 1$. Then

$$\begin{aligned} \sum_{j=1}^{n+1} \frac{(2j)!!}{(2j+1)!!} &= \frac{(2n+2)!!}{(2n+3)!!} + \sum_{j=1}^n \frac{(2j)!!}{(2j+1)!!} \\ &\stackrel{\text{IA}}{=} \frac{(2n+2)!!}{(2n+3)!!} + \frac{(2n+2)!! - 2(2n+1)!!}{(2n+1)!!} \\ &= \frac{(2n+3+1)(2n+2)!! - 2(2n+3)!!}{(2n+3)!!} \\ &= \frac{(2n+4)!! - 2(2n+3)!!}{(2n+3)!!}, \end{aligned}$$

which completes the induction step, and we finish the proof by multiplying both sides with $(2n+3)!!$. \square

Lemma 3. Let p be an odd prime and let α, β be integers. For every integer $n \geq 1$ let $\mathcal{S}_n(\alpha, \beta)$ in \mathbb{Q}_p be defined by

$$(3.3) \quad \mathcal{S}_n(\alpha, \beta) := (2n+1)!! \sum_{j=1}^n \frac{\alpha j + \beta}{2j+1}.$$

Then $\mathcal{S}_p(\alpha, \beta) \in \mathbb{Z}_p$ and $\tilde{\mathcal{S}}_p(\alpha, \beta) = \alpha/2 - \beta$.

Proof. Each term of $\mathcal{S}_p(\alpha, \beta)$ will contain a factor p and thereby be an element in $p\mathbb{Z}_p$, except for the j th term where $j = (p-1)/2$ because then the factor p in the numerator will vanish due to a factor p in the denominator.

Hence, the only term of $\mathcal{S}_p(\alpha, \beta)$ not in $p\mathbb{Z}_p$ is

$$(3.4) \quad \frac{(2p+1)!!}{p} (\alpha((p-1)/2) + \beta) = (2p+1) \cdots (p+2)(p-2) \cdots 3 \cdot 1 ((p-1)\alpha/2 + \beta).$$

This is certainly an element in \mathbb{Z}_p . Put

$$\mathcal{C} = \frac{(2p+1)!!}{p}.$$

Then

$$\begin{aligned} \mathcal{C} &= (2p+1)(2p-1) \cdots (p+2)(p-2) \cdots 3 \cdot 1 \\ &= (p+p+1)(p+p-1) \cdots (p+4)(p+2)(p-2) \cdots 3 \cdot 1 \\ &\equiv (p+1)(p-1) \cdots 4 \cdot 2 \cdot (p-2)!! \pmod{p} \\ &\equiv (p+1)!!(p-2)!! \pmod{p} \\ &\equiv (p+1)(p-1)! \pmod{p}. \end{aligned}$$

By Wilson's theorem we know that $(p-1)! \equiv -1 \pmod{p}$ and from this we deduce

$$(3.5) \quad \tilde{\mathcal{C}} = -1.$$

From (3.4) and (3.5) we then obtain

$$\tilde{\mathcal{S}}_p(\alpha, \beta) = \alpha/2 - \beta.$$

This completes the proof of Lemma 3. \square

An important part of the proof of Proposition 1 is utilization of the following lemma, which is a generalization of a lemma from [Ela05] to hold for any field k .

Lemma 4. [Ela05, §1.2] *Let k be a field. Furthermore let $f, g : \mathbb{Z}^+ \mapsto k$, and $y_0 \in k$. Given a nonhomogeneous difference equation*

$$y_{n+1} = f(n)y_n + g(n), y_{n_0} = y_0$$

where $n_0 \in [0, n]$. The general solution to the difference equation is given by

$$(3.6) \quad y_n = \left[\prod_{j=n_0}^{n-1} f(j) \right] y_0 + \sum_{r=n_0}^{n-1} \left[\prod_{j=r+1}^{n-1} f(j) \right] g(r).$$

Proof. This will be proved using induction. Assuming that (3.6) holds for some n , we now prove it for $n+1$. We have

$$y_{n+1} = f(n)y_n + g(n).$$

Substitution of y_n with the induction assumption yields

$$\begin{aligned}
y_{n+1} &= f(n) \left[\left[\prod_{j=n_0}^{n-1} f(j) \right] y_0 + \sum_{r=n_0}^{n-1} \left[\prod_{j=r+1}^{n-1} f(j) \right] g(r) \right] + g(n) \\
&= f(n) \left[\prod_{j=n_0}^{n-1} f(j) \right] y_0 + f(n) \sum_{r=n_0}^{n-1} \left[\prod_{j=r+1}^{n-1} f(j) \right] g(r) \\
&= \left[\prod_{j=n_0}^n f(j) \right] y_0 + \sum_{r=n_0}^n \left[\prod_{j=r+1}^n f(j) \right] g(r),
\end{aligned}$$

which completes the induction step. \square

Proof of Proposition 1. The proof of this proposition is divided into three parts. In the first part we define a recurrence relation Δ_m with the property that $\Delta_p = g^p(\zeta) - \zeta$, a method also used in e.g. [RL03], [LRL16b], and find the difference equations that defines the first three significant terms in Δ_m . In the second part we solve these difference equations for an arbitrarily chosen m , and in the last part we determine the coefficient of the first significant term in Δ_p and hence of $g^p(\zeta) - \zeta$.

Part 1. Finding the Difference Equations. Analogous to [LRL16b] for $m = 1$ we define the recurrence relation $\Delta_1(\zeta) := g(\zeta) - \zeta$ and for $m \geq 2$

$$\Delta_m(\zeta) := \Delta_{m-1}(g(\zeta)) - \Delta_{m-1}(\zeta).$$

Note that $\Delta_p(\zeta) = g^p(\zeta) - \zeta$. For technical reasons we define $G_\infty := \mathbb{Q}_p[x_2, x_3, \dots]$, and for each integer $\ell \geq 1$ put $G_\ell := \mathbb{Q}_p[x_2, x_3, \dots, x_\ell]$. Moreover we consider the power series $\hat{g} \in G_\infty[[\zeta]]$ defined as

$$\hat{g}(\zeta) := \zeta(1 + x_2\zeta^2 + x_3\zeta^3 + x_4\zeta^4) \mod \langle \zeta^6 \rangle.$$

For $m = 1$ we define the relation $\hat{\Delta}_1(\zeta) := \hat{g}(\zeta) - \zeta$ and for each integer $m \geq 2$

$$\hat{\Delta}_m(\zeta) := \hat{\Delta}_{m-1}(\hat{g}(\zeta)) - \hat{\Delta}_{m-1}(\zeta).$$

Defined in this way there is a clear relation between $g(\zeta)$ and $\hat{g}(\zeta)$ and thus between Δ_m and $\hat{\Delta}_m$. In the last part of the proof we exploit this relation to find the coefficients of $g^p(\zeta) - \zeta$.

Concerning $\widehat{\Delta}_2(\zeta)$, we have

$$\begin{aligned}
\widehat{\Delta}_2(\zeta) &= \widehat{\Delta}_1(\widehat{g}(\zeta)) - \widehat{\Delta}_1(\zeta) \\
&= x_2(\zeta + x_2\zeta^3 + x_3\zeta^4 + x_4\zeta^5 + x_5\zeta^6 + \dots)^3 \\
&\quad + x_3(\zeta + x_2\zeta^3 + x_3\zeta^4 + x_4\zeta^5 + x_5\zeta^6 + \dots)^4 \\
&\quad + x_4(\zeta + x_2\zeta^3 + x_3\zeta^4 + x_4\zeta^5 + x_5\zeta^6 + \dots)^5 \\
&\quad + x_5(\zeta + x_2\zeta^3 + x_3\zeta^4 + x_4\zeta^5 + x_5\zeta^6 + \dots)^6 + \dots - \Delta_1(\zeta) \\
&\equiv x_2\zeta^3 + 3x_2^2\zeta^5 + 3x_2x_3\zeta^6 + \left(\binom{3}{2}x_2^3 + 3x_2x_4\right)\zeta^7 + x_3\zeta^4 + 4x_2x_3\zeta^6 + 4x_3^2\zeta^7 \\
&\quad + x_4\zeta^5 + 5x_2x_4\zeta^7 + x_5\zeta^6 + x_6\zeta^7 - \widehat{\Delta}_1(\zeta) \pmod{\langle \zeta^8 \rangle} \\
&\equiv 3x_2^2\zeta^5 + 7x_2x_3\zeta^6 + \left(\binom{3}{2}x_2^3 + 4x_3^2 + 8x_2x_4\right)\zeta^7 \pmod{\langle \zeta^8 \rangle}.
\end{aligned}$$

We will see that it is necessary to keep track of the three first significant terms since $\text{ord}(\widehat{\Delta}_{m+1}(\zeta)) = \text{ord}(\widehat{\Delta}_m(\zeta)) + 2$ for $m \in \{1, \dots, p-1\}$. Note that neither the x_5 -nor the x_6 -term is affecting the first three significant terms.

Let $x = (x_2, x_3, \dots)$, more generally for a given $m \in \{1, \dots, p\}$ we have

$$(3.7) \quad \widehat{\Delta}_m(\zeta) = A_m(x)\zeta^{2m+1} + B_m(x)\zeta^{2m+2} + C_m(x)\zeta^{2m+3} + \dots,$$

where $A_m(x), B_m(x), C_m(x) \in G_\infty$. Throughout the rest of this proof let $A_m := A_m(x), B_m := B_m(x)$ and $C_m := C_m(x)$ unless otherwise specified. Defined in this manner the polynomials can be described by the following system of linear difference equations represented as follows

$$(3.8) \quad \begin{bmatrix} x_2(2m+1) & 0 & 0 \\ x_3(2m+1) & x_2(2m+2) & 0 \\ (x_2^2m+x_4)(2m+1) & x_3(2m+2) & x_2(2m+3) \end{bmatrix} \begin{bmatrix} A_m \\ B_m \\ C_m \end{bmatrix} = \begin{bmatrix} A_{m+1} \\ B_{m+1} \\ C_{m+1} \end{bmatrix},$$

with the initial conditions $(A_1, B_1, C_1) = (x_2, x_3, x_4)$. To see that this actually describes the situation we study $\widehat{\Delta}_{m+1}(\zeta)$ and obtain

$$\begin{aligned}
\widehat{\Delta}_{m+1}(\zeta) &= \widehat{\Delta}_m(\widehat{g}(\zeta)) - \widehat{\Delta}_m(\zeta) \\
&= \widehat{\Delta}_m(\zeta + x_2\zeta^3 + x_3\zeta^4 + x_4\zeta^5 + x_5\zeta^6 + \dots) - \widehat{\Delta}_m(\zeta) \\
&= A_m(\zeta + x_2\zeta^3 + x_3\zeta^4 + x_4\zeta^5 + x_5\zeta^6 + \dots)^{2m+1} \\
&\quad + B_m(\zeta + x_2\zeta^3 + x_3\zeta^4 + x_4\zeta^5 + x_5\zeta^6 + \dots)^{2m+2} \\
&\quad + C_m(\zeta + x_2\zeta^3 + x_3\zeta^4 + x_4\zeta^5 + x_5\zeta^6 + \dots)^{2m+3} + \dots - \widehat{\Delta}_m(\zeta) \\
&\equiv A_mx_2(2m+1)\zeta^{2m+3} + A_mx_3(2m+1)\zeta^{2m+4} + A_m\left(x_2^2\binom{2m+1}{2} + x_4(2m+1)\right)\zeta^{2m+5} \\
&\quad + B_mx_2(2m+2)\zeta^{2m+4} + B_mx_3(2m+2)\zeta^{2m+5} + C_mx_2(2m+3)\zeta^{2m+5} \pmod{\langle \zeta^{2m+6} \rangle} \\
&\equiv A_mx_2(2m+1)\zeta^{2m+3} + (A_mx_3(2m+1) + B_mx_2(2m+2))\zeta^{2m+4} \\
&\quad + (A_m((2m+1)(x_2^2m+x_4)) + B_mx_3(2m+2) + C_mx_2(2m+3))\zeta^{2m+5} \pmod{\langle \zeta^{2m+6} \rangle}.
\end{aligned}$$

This in fact implies that $A_m, B_m, C_m \in G_4$. The next step of the proof is to find a closed form expression of these polynomials after m iterations

Part 2. Solving the Difference Equations. In this section we discuss the solutions to the difference equations (3.8) given in the previous section. First note that since \mathbb{Q}_p is a field and the equations in (3.8) are linear there are unique solutions $\{A_m\}_{m \geq 1}$, $\{B_m\}_{m \geq 1}$ and $\{C_m\}_{m \geq 1}$ respectively. Also note that all three difference equations are first order, and except for A_m they are nonhomogeneous.

We now apply Lemma 4 to solve the equations. We start by considering the top equation in (3.8)

$$A_{m+1} = x_2(2m+1)A_m, \quad A_1 = x_2.$$

Considering Lemma 4 we obtain the solution

$$(3.9) \quad A_m = \left[\prod_{j=1}^{m-1} x_2(2j+1) \right] A_1 = x_2^{m-1}(2m-1)!!x_2 = x_2^m(2m-1)!!.$$

Now we have the solution to our first difference equation and insertion into B_m in (3.8) yields

$$(3.10) \quad \begin{aligned} B_{m+1} &= x_2(2m+2)B_m + x_3(2m+1)A_m \\ &= x_2(2m+2)B_m + x_3(2m+1)x_2^m(2m-1)!! \\ &= x_2(2m+2)B_m + x_2^m x_3(2m+1)!!. \end{aligned}$$

Now we can see that B_m is in fact a nonhomogeneous difference equation. We utilize substitution to obtain a simpler expression. Assuming $x_3 \neq 0$ this yields

$$(3.11) \quad B_{m+1}^* = \frac{B_{m+1}}{x_2^m x_3(2m+1)!!}.$$

Insertion of (3.11) into (3.10) yields

$$x_2^m x_3(2m+1)!!B_{m+1}^* = x_2^m x_3(2m+2)(2m-1)!!B_m^* + x_2^m x_3(2m+1)!!,$$

hence

$$B_{m+1}^* = \frac{2m+2}{2m+1}B_m^* + 1.$$

Note that $B_1 = x_3$ implies that $B_1^* = 1$ from (3.11). Now we can solve B_m^* using Lemma 4 and we obtain

$$\begin{aligned} B_m^* &= \left[\prod_{j=1}^{m-1} \frac{2j+2}{2j+1} \right] B_1^* + \sum_{r=1}^{m-1} \left[\prod_{j=r+1}^{m-1} \frac{2j+2}{2j+1} \right] \\ &= \sum_{r=1}^m \left[\prod_{j=r+1}^m \frac{2j}{2j-1} \right]. \end{aligned}$$

Substitution of B_m^* in (3.11) for B_m together with the definition of \mathcal{R}_m in Lemma 2 yields

$$(3.12) \quad \begin{aligned} B_m &= x_2^{m-1} x_3(2m-1)!! \sum_{r=1}^m \left[\prod_{j=r+1}^m \frac{2j}{2j-1} \right] \\ &= x_2^{m-1} x_3 \mathcal{R}_m \\ &= x_2^{m-1} x_3 ((2m+1)!! - (2m)!!). \end{aligned}$$

Hence, we have a solution for B_m as well which means that we can express C_m (the last equation in (3.8)) as a nonhomogeneous difference equation depending solely on C_m and m . Inserting the solutions for A_m and B_m , (3.9) and (3.12) respectively into (3.8) with initial value $C_1 = x_4$ and for $m \geq 1$ we have

$$\begin{aligned}
 (3.13) \quad C_{m+1} &= x_2^m (2m-1)!! ((2m+1)(x_2^2 m + x_4)) \\
 &\quad + 2(m+1)x_2^{m-1} x_3^2 ((2m+1)!! - (2m)!!) + x_2(2m+3)C_m \\
 &= x_2^{m+2} m(2m+1)!! + x_2^m x_4 (2m+1)!! \\
 &\quad + 2(m+1)x_2^{m-1} x_3^2 ((2m+1)!! - (2m)!!) + x_2(2m+3)C_m.
 \end{aligned}$$

Since this is a linear difference equation we simplify this problem by splitting this equation into three separate equations. For $m \geq 1$ we define D_m, E_m and F_m as

$$(3.14) \quad \begin{bmatrix} x_2(2m+3)D_m \\ x_2(2m+3)E_m \\ x_2(2m+3)F_m \end{bmatrix} + \begin{bmatrix} d(m) \\ e(m) \\ f(m) \end{bmatrix} = \begin{bmatrix} D_{m+1} \\ E_{m+1} \\ F_{m+1} \end{bmatrix},$$

with the initial conditions $(D_1, E_1, F_1) = (0, x_4, 0)$.

Furthermore, let

$$\begin{aligned}
 d(m) &= x_2^{m+2} m(2m+1)!! \\
 e(m) &= x_2^m x_4 (2m+1)!! \\
 f(m) &= 2(m+1)x_2^{m-1} x_3^2 ((2m+1)!! - (2m)!!),
 \end{aligned}$$

and thereby equation (3.13) is satisfied. This can be seen as follows

$$\begin{aligned}
 D_{m+1} + E_{m+1} + F_{m+1} &= x_2(2m+3)D_m + d(m) + x_2(2m+3)E_m \\
 &\quad + e(m) + x_2(2m+3)F_m + f(m) \\
 &= x_2(2m+3)(D_m + E_m + F_m) + d(m) + e(m) + f(m) \\
 &= x_2(2m+3)(C_m) + d(m) + e(m) + f(m) \\
 &= C_{m+1}.
 \end{aligned}$$

By solving D_m, E_m and F_m separately we can retrieve the solution to C_m .

We start by finding the solution for

$$(3.15) \quad D_{m+1} = x_2(2m+3)D_m + x_2^{m+2} m(2m+1)!!.$$

Analogous with (3.11) we utilize substitution

$$D_{m+1}^* = \frac{D_{m+1}}{x_2^{m+2} (2m+3)!!}.$$

Insertion into (3.15) yields

$$D_{m+1}^* = D_m^* + \frac{m}{2m+3},$$

and since $D_1^* = 0$ this means that for every iteration of the recursion the fraction term will add on. This yields a solution of the form

$$D_m^* = \sum_{j=1}^{m-1} \frac{j}{2j+3} = \sum_{j=1}^m \frac{j-1}{2j+1}.$$

Changing variable back to D_m we get that

$$(3.16) \quad D_m = x_2^{m+1}(2m+1)!! \sum_{j=1}^m \frac{j-1}{2j+1}.$$

The difference equation for E_m is given by

$$(3.17) \quad E_{m+1} = x_2(2m+3)E_m + x_2^m x_4(2m+1)!!.$$

Substitution gives us

$$E_{m+1}^* = \frac{E_{m+1}}{x_2^m(2m+3)!!},$$

which then yields

$$(3.18) \quad E_{m+1}^* = E_m^* + \frac{x_4}{2m+3}.$$

By utilizing Lemma 4 the solution to (3.18) is given by,

$$E_m^* = \frac{x_4}{3} + \sum_{j=1}^{m-1} \frac{x_4}{2j+3} = x_4 \sum_{j=1}^m \frac{1}{2j+1},$$

which means that the solution to (3.17) is

$$(3.19) \quad E_m = x_2^{m-1} x_4(2m+1)!! \sum_{j=1}^m \frac{1}{2j+1}.$$

The difference equation for F_m is given by

$$(3.20) \quad F_{m+1} = x_2(2m+3)F_m + 2(m+1)x_2^{m-1}x_3^2((2m+1)!! - (2m)!!).$$

Assume that $x_3 \neq 0$, and furthermore as in the previous case for D_m we use substitution, and obtain

$$F_{m+1}^* = \frac{F_{m+1}}{x_2^{m-1}x_3^2(2m+3)!!}.$$

Inserting this into (3.20) yields

$$F_{m+1}^* = F_m^* + (2m+2) \left(\frac{(2m+1)!! - (2m)!!}{(2m+3)!!} \right) \iff F_{m+1}^* = F_m^* + \frac{2m+2}{2m+3} - \frac{(2m+2)!!}{(2m+3)!!}.$$

By the same reasoning as above, since $F_1^* = 0$, we have

$$F_m^* = \sum_{j=1}^{m-1} \left[\frac{2j+2}{2j+3} - \frac{(2j+2)!!}{(2j+3)!!} \right] = \sum_{j=1}^m \left[\frac{2j}{2j+1} - \frac{(2j)!!}{(2j+1)!!} \right],$$

which means that the solution to our original equation is

$$(3.21) \quad F_m = x_2^{m-2} x_3^2(2m+1)!! \sum_{j=1}^m \left[\frac{2j}{2j+1} - \frac{(2j)!!}{(2j+1)!!} \right].$$

Consequently, by summing (3.16), (3.19) and (3.21) we obtain

$$\begin{aligned}
 (3.22) \quad C_m &= D_m + E_m + F_m \\
 &= x_2^{m+1}(2m+1)!! \sum_{j=1}^m \frac{j-1}{2j+1} \\
 &\quad + x_2^{m-1}x_4(2m+1)!! \sum_{j=1}^m \frac{1}{2j+1} \\
 &\quad + x_2^{m-2}x_3^2(2m+1)!! \sum_{j=1}^m \left[\frac{2j}{2j+1} - \frac{(2j)!!}{(2j+1)!!} \right].
 \end{aligned}$$

Together with (3.9) and (3.12) we now have closed form expressions of the coefficients in (3.7).

Part 3. Determining the coefficients of $g^p(\zeta) - \zeta$. Recall that

$$\widehat{g}^p(\zeta) - \zeta = A_p \zeta^{2p+1} + B_p \zeta^{2p+2} + C_p \zeta^{2p+3} \pmod{\langle \zeta^{2p+4} \rangle}.$$

It follows from (3.9) and (3.12) that $A_p, B_p \in \mathbb{Z}_p[x_2, x_3, x_4]$. In particular,

$$(3.23) \quad \widetilde{A}_p = \widetilde{B}_p = 0.$$

Using the definitions of \mathcal{S}_p and \mathcal{T}_p from Lemma 2 and 3 together with (3.22) we have

$$C_p = x_2^{p+1}\mathcal{S}_p(1, -1) + x_2^{p-1}x_4\mathcal{S}_p(0, 1) + x_2^{p-2}x_3^2(\mathcal{S}_p(2, 0) - \mathcal{T}_p).$$

Also note that by Lemma 2 and 3 we have

$$\widetilde{\mathcal{S}}_p(1, -1) = 3/2, \quad \widetilde{\mathcal{S}}_p(0, 1) = -1, \quad \widetilde{\mathcal{S}}_p(2, 0) = 1, \quad \text{and} \quad \widetilde{\mathcal{T}}_p = 0.$$

Consequently,

$$\widetilde{C}_p(x_2, x_3, x_4) = x_2^{p-2}(3/2x_2^3 + x_3^2 - x_2x_4).$$

Finally, for each $i \geq 1$ we specialize each variable x_i to a_i and obtain

$$(3.24) \quad \widetilde{C}_p(a_2, a_3, a_4) = a_2^{p-2}(3/2a_2^3 + a_3^2 - a_2a_4).$$

We conclude that

$$\begin{aligned}
 g^p(\zeta) - \zeta &= \widetilde{C}_p(a_2, a_3, a_4)\zeta^{2p+3} \pmod{\langle \zeta^{2p+4} \rangle} \\
 &= a_2^{p-2}(3/2a_2^3 + a_3^2 - a_2a_4)\zeta^{2p+3} \pmod{\langle \zeta^{2p+4} \rangle}.
 \end{aligned}$$

This completes the proof of Proposition 1. \square

Proof of Theorem 1. Assuming that $a_1 = 0$, $a_2 \neq 0$ and $3/2a_2^3 + a_3^2 - a_2a_4 \neq 0$, then we obtain by the assumption that $i_0(g) = 2$, and by Proposition 1 that $i_1(g) = 2(1+p)$, together with [LS98, Corollary 1] this implies that g is 2-ramified. Conversely, assuming that g is 2-ramified then by Proposition 1 we obtain $3/2a_2^3 + a_3^2 - a_2a_4 \neq 0$. We also recall that if g is 2-ramified then $i_0(g) = 2$, which in turn implies that $a_1 = 0$ and $a_2 \neq 0$. \square

3.1. Proof of implication. We give a proof to Corollary 1, stated in §1.1.

Proof of Corollary 1. We compute $f^2(\zeta)$ explicitly. Recall that

$$f(\zeta) = \zeta(-1 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4) \pmod{\langle \zeta^6 \rangle},$$

which yields

$$f^2(\zeta) = \zeta - 2(a_1^2 + a_2)\zeta^3 + (a_1^3 + a_1a_2)\zeta^4 + (3a_2^3 - 6a_1a_3 - a_1^2a_2 - 2a_4)\zeta^5 \pmod{\langle \zeta^6 \rangle}.$$

Using Theorem 1 we have that f^2 is 2-ramified if and only if (1.5) holds. This yields

$$\begin{aligned} & \frac{1}{2}(-2a_1^2 - 2a_2)^{p-2}(3(-2a_1^2 - 2a_2)^3 + 2(a_1^3 + a_1a_2)^2 \\ & \quad - 2(-2a_1^2 - 2a_2)(3a_2^3 - 6a_1a_3 - a_1^2a_2 - 2a_4)) \\ & = -(-2a_1^2 - 2a_2)^{p-2}(a_1^2 + a_2)(11a_1^4 + 25a_1^2a_2 + 12a_1a_3 + 6a_2^2 + 4a_4) \\ & = 2^{p-2}(a_1^2 + a_2)^{p-1}(11a_1^4 + 25a_1^2a_2 + 12a_1a_3 + 6a_2^2 + 4a_4), \end{aligned}$$

which proves our corollary. \square

REFERENCES

- [AK09] Vladimir Anashin and Andrei Khrennikov. *Applied algebraic dynamics*. Walter De Gruyter, Berlin, 2009.
- [Ela05] Saber Elaydi. *An introduction to difference equations*. Springer, New York, 3. ed. edition, 2005.
- [Kea92] Kevin Keating. Automorphisms and extensions of $k((t))$. *Journal of Number Theory*, 41(3):314–321, 1992.
- [Lin13] Karl-Olof Lindahl. The size of quadratic p -adic linearization disks. *Adv. Math.*, 248:872–894, 2013.
- [LMS02] François Laubie, Abbas Movahhedi, and Alain Salinier. Systèmes dynamiques non archimédiens et corps des normes. *Compositio Mathematica*, 132(1):57–98, 2002.
- [LRL16a] Karl-Olof Lindahl and Juan Rivera-Letelier. Generic parabolic points are isolated in positive characteristic. *Nonlinearity*, 29(5):1596–1621, 2016.
- [LRL16b] Karl-Olof Lindahl and Juan Rivera-Letelier. Optimal cycles in ultrametric dynamics and minimally ramified power series. *Compos. Math.*, 152(1):187–222, 2016.
- [LS97] François Laubie and M. Saïne. Ramification of automorphisms of $k((t))$. *Journal of Number Theory*, 63(1):143–145, 1997.
- [LS98] François Laubie and M. Saïne. Ramification of Some Automorphisms of Local Fields. *Journal of Number Theory*, 72(2):174–182, 1998.
- [Lub94] Jonathan Lubin. Non-Archimedean dynamical systems. *Compositio Math.*, 94(3):321–346, 1994.
- [Lub95] Jonathan Lubin. Sen’s theorem on iteration of power series. *Proceedings of the American Mathematical Society*, 123(1):63–66, 1995.
- [RL03] Juan Rivera-Letelier. Dynamique des fonctions rationnelles sur des corps locaux. *Astérisque*, 287(xv):147–230, 2003.
- [Sen69] Shankar Sen. On automorphisms of local fields. *Ann. of Math. (2)*, 90:33–46, 1969.
- [Shp07] Igor E. Shparlinski. On some dynamical systems in finite fields and residue rings. *Discrete Contin. Dyn. Syst.*, 17(4):901–917, 2007.
- [Sil07] Joseph H. Silverman. *The arithmetic of dynamical systems*. Springer, New York, N.Y., 2007.
- [Win04] Jean-Pierre Wintenberger. Automorphismes des corps locaux de caractéristique p . *J. Théor. Nombres Bordeaux*, 16(2):429–456, 2004.